IN THE SPECIFICATION

Kindly amend the specification according to the following listing of paragraphs from the publication (US 2010/0199189):

Please delete Paragraph [0034] and insert the following replacement paragraph [0034]:

[0034] Referring now to FIG. 1, showing a schematic block diagram of a preferred embodiment of the disclosed invention. The interactions are intercepted at one or more front ends and are transferred to a back end. The exemplary embodiment includes front end 10 relating to telephony, front end 20 relating to an internet service provider and front end 30, relating to a general switch, presented here for demonstrating a non-specific front end. The apparatus further comprises back end 50. Each front end preferably supports multiple criteria for multiple back ends. For example, different law enforcement authorities can apply separate rules regarding separate numbers, and the calls relevant for each authority will be transferred to the back end of the relevant authority. Front end 10 relates to intercepting telephone or fax interactions. Front end 10 comprises a telephony switchboard 14 of a commercially available type such as those produced by Ericsson, Nortel, Motorola, Cisco, or the like, through which all interactions pass. Alternatively, switchboard 14 can be replaced by a component of a switch, or a component joined to the switch that enables the transfer of calls. Front end 10 further comprises a mediation component 16 which applies one or more interception criteria as set and defined by one or more users as will be detailed in association with the back end below. The interception criteria can include raw data such as calling number, dialed number, location, IMSI, IMEI, application (for example e-mail, http, web page or the like), port, IP address, Internet MAC address or call metadata, or data which is a result of further processing, such as identified language based in audio or text, keyword comprised in text, speaker identified by voice print or other data related to the content of the interaction. In some cases which are more likely to be intelligence-related than law-enforcement related the interception criteria can further include more complex conditions, available from the data of the interaction itself, and not from the meta data available from the switchboard. Such data can include words spotted within the interaction, a certain

speaker identified as a participant in an interaction, an emotional level within a telephone interaction, a certain data item within a fax, or another feature that can be identified within an interaction. In the case of speaker identification, another added value of using the engine is the minimization of monitored and captured communications, i.e. determining whether the communication item complies with an interception criteria anytime during the interaction and not just at the beginning. For example, in some law enforcement organizations, recording is allowed only of the suspect himself, and only in calls related to the suspicions. Identifying the speaker throughout or anytime during the interaction enables a listener to start listening and possibly recording as soon as the target himself starts speaking, thus avoid missing the call because another person started the conversation as is often done by law-aware targets.

Please delete Paragraph [0039] and insert the following new paragraph [0039]:

[0039] Referring now to FIG. 2, showing the main steps of the method of the disclosed invention, preferably as used with the apparatus of FIG. 1. The first step of the method is hierarchy definition step 66. The hierarchy comprises one or more cases, sub cases, targets and interception criteria (IC). The ICs are optionally derived from and are in accordance with one or more warrants. Each IC is applied at one or more front end, such as a switchboard of a telephony company, a site of an internet service provider (ISP) or the like. Warrant-driven interception is more related to law-enforcement agencies, and non-warrant-related is more typical of intelligence systems, but this division is not binding. At the front end, for each communication it is determined at step 70 whether the communication complies with the IC. Some of the IC's conditions, such as phone number or time are compared against the IRI or another external source of information, and some are determined from the content of the communication itself, by performing analysis step 76. If the communication is determined to comply with the IC, it is captured at step 74. Since step 76 requires at least part of the communication, if there is a chance that the communication should be intercepted, it is captured at step 74, analyzed at step 76, and if determined to comply with the IC, it is passed at step 75 to the back end. If the communication does not comply with the IC, it is discarded. Analysis step 76 can comprise any type of analysis relevant for the captured communication. Voice communications can be

analyzed by engines including automatic transcription, word spotting, speaker identification, speaker verification, speaker hunting, speaker recognition, phonetic search, language identification, emotion detection, and others; communication items such as fax transmitted can be analyzed using object character recognition (OCR); textual communication is optionally analyzed using any of the following: language identification, free text search, categorization, clustering, entity tagging and relationship, automatic summary, translation, or the like; internet browsing sessions are optionally captured according to the relevant warrants, for example all browsing or only to specific sites, and similarly for additional types of communication currently known or that will become known in the future. Link analysis and data mining can also be performed on relevant information. In cases wherein interception and capturing is limited, due for example to a limiting warrant limiting capturing hours or dates, or specific web addresses, the relevant logic is applied at step 70. However, step 76 can be skipped at the front end, such that all communications whose IRI comply with one or more ICs are passed to the backend. If step 76 is performed, the analysis results are passed together with the content and the IRI to the backend at step 75. At the backend, the communications are optionally reviewed at reviewing step 78. At reviewing step 78, the user is presented with the case hierarchy or with one or more communication items, and can listen to vocal communications or to one side of the communication item, view their contents, add comments, add action items, assign a communication to another user and additional operations. The user can view a textual presentation of a textual communication item or a pictorial presentation of an image, such as a fax communication. Some of the communications might be directed by a user to analysis step 76 as performed at the back end. The analysis engines used at the backend may be the same, utilize different parameters or be altogether different from the analysis engines used at the front end. The communication analysis may be human or automated. For example, a human operator can listen to calls, while an automated system can search for spotted words. The products or results of reviewing step 78 or communication analysis step 76 are optionally fed back into interception criteria determination step 70, for deleting, enhancing or changing one or more interception criteria based on actual captured communications. For example, if an interception criteria involves an e-mail address, when a user is using the address from a certain computer, the IP address of the computer can be captured, and additional interception criteria, such as an additional e-mail addresses used from this computer,

can be added as an interception criteria. Another example involves IP expansion of the IP address of a computer, out of which a target sent a text file containing a certain word. Reviewing step 78 or communication analysis step 76 comprise a set of rules according to which it is decided which criteria are fed back into, and for how long. For example, if a target used an internet cafe, the next person using the same computer is not likely to be a target.

Please delete Paragraph [0041] and insert the following new paragraph [0041]:

[0041] Referring now to FIGS. 3 to 13, showing various aspects of a preferred embodiment of the apparatus. FIGS. 3 to 13 are illustrations of possible computer screenshots of a preferred computerized embodiment of the disclosed invention. However, FIGS. 3 to 13 shown and explained below are exemplary only and serve merely to present and exemplify the underlying principles and methods of the disclosed invention. Persons skilled in the art will appreciate that different implementations, regarding the internals of the system, as well as its user-interface aspects can be implemented in various ways utilizing different technologies and methodologies. With the present implementation, the user can obtain within a glance as much information as possible regarding one or more interception communications, targets or other entities in the system. Mode selection bar 104 of FIG. 3 allows a user to select the mode he or she wishes to work in, subject to the user's profile (operational, management, etc.) and the allowed permissions. In FIG. 3, the user selected "Monitoring" mode by pressing button 108 and is working in monitoring mode, which provides a user-customizable display of intercepted interactions in real time or near-real-time. Area 112 of FIG. 3 shows a graphic representation of the investigations hierarchy. The top level of the hierarchy is a case, such as smuggling 116 or fraud 120, which is the parent entity which comprises one or more subjects for interception under the same investigation. Each case may comprise one or more sub-cases, such as sub case 1 124 or sub case 2 128, each sub-case regarding a subject of more focused work effort. For example, within a homicide case there may a focused investigation on a particular group of suspects. However, sub-cases are not a mandatory component in the hierarchy and can be skipped. The third level is the target, such as Victor 132 or Mike stone 136 in FIG. 3. A target is usually an

individual, whose communications are marked for interception. Each target can be intercepted using one or more communication channels, such as phone, fax, computer, cellular phone or the like. The last level is the interception criteria (IC), such as Victor's computer 140, Victor's fixed line 144, or Victor's phone 148, all of FIG. 3. Next to each row in each level, the system denoted in parenthesis 124 the total number of items, (such as audio captures, video captured, e-mail messages and the like) collected at this level and its sub-levels, and the accumulated duration of audio or video captured interactions, which is important for the user for estimating the time it will take to analyze the captured material. Each IC is usually a combination of one or more parameters relating to a certain communication channel, defining which communication items are to be intercepted. An IC can relate to: one or more phone lines, possibly involving limitations such as times, dates, called number or the like; the international mobile subscriber identity (IMSI) or international mobile station equipment identity (IMEI) of a cellular phone; an e-mail address; an IP address; or other identifiers of telecommunication channels. Each one or more presented interception criteria are associated with one or more interception criteria in a back end unit. The ICs are optionally related to warrants issued by court, which authorize eavesdropping to the target. The ICs are constructed, as will be detailed below, in connection to the warrants, if available. Each component in the hierarchy, i.e. a case, sub-case, target, and IC can be associated and displayed to one or more users, and each user can view any number of hierarchy components. The components viewed by a user are determined according to a security and privileges policy, and profile definition. Profiles within the apparatus can include administrative profiles, operational profiles or master profiles, thus determining the privileges. Each user can be associated with multiple profiles, according to his or her role in one or more investigations. A checkmark such as 152 next to an item in the hierarchy indicates that the relevant item and all its sub-items, unless unchecked, are active, meaning that all checked interception criteria are active at the relevant IC operation components at the relevant front ends. The hierarchy view is preferably enabled in all modes and for all users, however, the contents presented to each user vary according to the profile, the privileges and the assignments assigned to the user. The upper right hand side pane of the screenshot, generally referred as 156 shows relevant details for each activity associated with the checked case, sub-case, target, or IC and their sub-entities in the hierarchy (e.g. all ICs under a certain checked target, all targets and all

associated ICs under a checked sub-case, etc.). The relevant information includes identification and technical data, such as event ID 160, event type (telephone, fax, etc.) 164, target name 168, event direction (incoming or outgoing) 172, the other party's name (OP) 176, start time 180, IC type 184, IC name 188, and an indication 192 whether the interaction is currently active. In addition, indicators 250 and 254 indicate whether there are any ~~and~~ active or urgent events currently going on. Although the communications are of different types, the presentation is unified, using uniform parameters, thus enabling a user to efficiently grasp the occurrences. It is possible to define communications complying with certain ICs as requiring smart-alerts, meaning that when a new interaction was captured and is being transmitted, a pop-up window will appear on the screen, notifying the investigator about the new activity, as shown in pop-~~p~~up window 300 of FIG. 4, comprising information about the event and options for the user, such as reminding in a predetermined time 304, snooze 308, dismiss 312, and go-to-event 316. Referring now back to FIG. 3, the lower right hand side, generally referred to as 200 of the screen provides a number of ways to view additional information related to highlighted interaction 204 in the upper right hand side pane. Vocal events, regardless of their origin, are preferably viewed using a playback module such as the one shown in FIG. 3. When the selected tab of tab buttons 208 is "playback", a voice communication can be played either offline or in real-time. Real-time monitoring uses voice over IP technology. The playback module supports a wide range of playback types: stereo playback, wherein each side of the call is displayed on a separate bar, such as target bar 206 and other party bar 207, and has a separate volume control; Mixed playback, where both sides of the call are mixed into a single channel; or synchronized playback, wherein two calls can be played simultaneously, either mixed or separated. The available playback control features include: play/stop 212; pause/resume 220; jump forward/backward 216/224; loop playback of a certain period; jump anywhere within the call by pointing at the time bar; target volume control 228 and other-party volume control 232; or skip silence. The playback screen, can also present additional information, either automatically derived information such as words spotted in the voice by a word spotting engine or segments of high emotions, or user-entered data, such as comments 236, a picture of the target or the other party, a time tag, a manually entered transcription or the like. In addition, preferably in processing mode, the user is allowed to associate any of the abovementioned user-entered information items with

the communication in general or with a specific point in time during the interaction, including memos, action items, or things to check. The playback screen can also present one or more IRI information items, such as transfer, hold, and the like. Referring now to FIG. 5, showing the system when the selected tab of tab list 208 is "content". With the "content" selection, a visual communication such as a fax or web browsing, in this case the fax transmission denoted as 404, is viewed as seen in pane 400 of FIG. 5. The contents are displayed by a viewer which can display the decoded image, the event's information or both. The intercepted images are preferably presented in TIFF format, enabling multiple pages to be wrapped up in a single file. The fax viewer enables users to perform a variety of operations on the decoded image, without manipulating the original image. The operations comprise zooming, rotating, inverting and other operations. When the transferred image is coded, presenting it as a TIFF image isn't ~~available~~ valuable. In such cases, the viewer offers the ability to view the image as raw binary data, enabling the decoding of the image by experts. The information related to the event comprises the signal level (in db); communication protocol; compression mode; error correction; sending fax; receiver fax and additional details. Area 400 can alternatively display e-mails or news events, which include beside their content, other important parameters, such as sender, receiver, subject, attachment etc. The events are preferably displayed using XML format, in order to enable their simple export to external systems. The looks and behavior of the viewer can resemble common e-mail viewers, such as MS Outlook, and the important parameters are displayed in a simple, easy to understand format, thus providing the user with a familiar environment. When the intercepted communication is an SMS, it can be viewed by an SMS viewer, displaying the contents of the SMS, as well as other relevant parameter, such as the SMS protocol, the encoding and the like. When the intercepted event is web browsing, the system's dedicated web viewer can presents the target's intercepted web browsing sessions in the same manner the target viewed them. This includes viewing JavaScript and ActiveX elements, and handling script-protected pages. "Cookies" downloaded from the web server to the target are displayed as well. When the intercepted communication is textual, such as a chat, a messenger session, an FTP or a telnet session, the content viewer actually shows a table in which every entry is displayed in a new row accompanied by its parameters such as time stamp, origin, type, etc. In case of file transfer (by FTP, DCC etc.) a link to the decoded file is displayed and the

file can be opened and viewed. This form simplifies user operations on the intercepted event; the user can easily sort the entries by time, type etc. and can apply a keyword search on the content.

Please delete Paragraph [0045] and insert the following new paragraph [0045]:

[0045] Other viewing options, such as the content or the map are available as in monitoring mode. Middle right hand pane 504 allows the user to enter keywords or synopsis upon which searching is then enabled. The apparatus can be further integrated with a speech-to-text engine or a translator for automatically transcribing or translating the interactions. Even if the quality of the transcription or translation generated by the automatic tools is not satisfactory, their output can still be used as a basis for manual enhancement. In processing mode the user is able to display all communications assigned to him in a list. ~~, enables the users to~~

Please delete Paragraph [0046] and insert the following new paragraph [0046]:

[0046] Yet another mode enabled by the apparatus is analysis mode, intended to be used by information analysts for obtaining further information from the intercepted communication items, the processes performed upon them and additional data entered by persons who worked with the information at an earlier stage. In analysis mode the user can create lists of communication items, assign the lists or parts thereof to people responsible to a certain aspect of an investigation, move, copy, or delete items. The user is also presented with an option to generate, save, run, and analyze different queries, as shown in FIG. 9, when the active tab of tab list 832 is "Queries" tab 836. A query can relate to any one or more data items associated with or contained within communications, including interception related information (IRI), such as duration or time range as indicated in 804 or 808 panes, respectively, location as indicated in pane 812, one or more participants selected in tab 816 of tab list 820, free search for words or phrases contained in a text communication, in a transcription or translation of a telephone interaction, in comments associated with the interaction, in the keywords or the synopsis of an interaction, or any combination of the above, as

indicated when using tab 824. The apparatus is preferably target-oriented, i.e., when a communication is presented, the target is clearly marked, even if he or she is not a main participant in the communication. For example, in e-mail messages, the target will be highlighted even if his name is in the CC or even BCC field, in a phone conversation it will be marked even if ~~of~~ the call was captured due to the other person, and the like. However, the queries can also relate to the other party talking with the target. The analyst can also use external visualization tools to obtain further aspects of the intercepted data or its IRI, define criteria for smart alerts, i.e., communications that require immediate attention, or additional tools. Smart alerts are not just interpreted for immediate use, but also stored for ongoing usage and continuous monitoring. The analyst can construct groups of queries as shown in upper left hand pane 828: public queries, private queries and others. The user can further create and use query templates.

Please delete Paragraph [0055] and insert the following new paragraph [0055]:

[0055] The system can further perform data retention, i.e. keep the IRI and utilize it at a later time, for purposes such as showing the locations of targets when performing communications on a map, deducing targets' patterns of behaviors and the like. In addition, it is also possible to introduce into the system external communications which were not intercepted by a front end of the system, such as TV recordings relating to a target, external recordings of phone conversations and others. The added communications can be analyzed and viewed similarly to the intercepted items. Certain targets or certain IC parameters, such as a VIP's phone line can be marked as belonging to a "white-list", i.e. a target not ~~tot~~ listened to, even when a target contacts them. Additionally, certain parameters can be marked as non-relevant, such as the number of an information service, the URL of a home page of a large portal or others.